# PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

## PCT

### NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

| | |
|---|---|
| **Date of mailing** (day/month/year)<br>03 January 2001 (03.01.01) | |
| **International application No.**<br>PCT/GB00/01354 | **Applicant's or agent's file reference**<br>Jg-2451-PCT |
| **International filing date** (day/month/year)<br>10 April 2000 (10.04.00) | **Priority date** (day/month/year)<br>26 April 1999 (26.04.99) |
| **Applicant**<br>KELMAN, Alistair, Bruce | |

1. The designated Office is hereby notified of its election made:

   [X] in the demand filed with the International Preliminary Examining Authority on:

   09 November 2000 (09.11.00)

   [ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

   [ ] was not

   made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

**The International Bureau of WIPO**
**34, chemin des Colombettes**
**1211 Geneva 20, Switzerland**

Facsimile No.: (41-22) 740.14.35

Authorized officer

Juan Cruz

Telephone No.: (41-22) 338.83.38

# PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

## PCT

To:

SANDERSON, Laurence, Andrew
Sanderson & Co.
34 East Stockwell Street
Colchester, Essex CO1 1ST
ROYAUME-UNI

## NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

**Date of mailing** (day/month/year)
13 November 2001 (13.11.01)

**Applicant's or agent's file reference**
6/LC/01-122

**IMPORTANT NOTIFICATION**

**International application No.**
PCT/GB00/01354

**International filing date** (day/month/year)
10 April 2000 (10.04.00)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address

JONES, Graham, Henry
Graham Jones & Company
77 Beaconsfield Road
Blackheath
London SE3 7LG
United Kingdom

State of Nationality:
State of Residence:
Telephone No.: 020 8858 4039
Facsimile No.: 020 8293 5920
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[X] the person [ ] the name [ ] the address [ ] the nationality [ ] the residence

Name and Address

SANDERSON, Laurence, Andrew
Sanderson & Co.
34 East Stockwell Street
Colchester, Essex CO1 1ST
United Kingdom

State of Nationality:
State of Residence:
Telephone No.:
Facsimile No.:
Teleprinter No.:

3. Further observations, if necessary:
**Also, please note the new reference number.**

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

**The International Bureau of WIPO**
**34, chemin des Colombettes**
**1211 Geneva 20, Switzerland**
Facsimile No.: (41-22) 740.14.35

Authorized officer
Idhir BRITEL
Telephone No.: (41-22) 338.83.38

# PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

## PCT

**NOTIFICATION OF THE RECORDING OF A CHANGE**

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

JONES, Graham, Henry
Graham Jones & Company
77 Beaconsfield Road
Blackheath
London SE3 7LG
ROYAUME-UNI

**Date of mailing** (day/month/year)
26 October 2001 (26.10.01)

**Applicant's or agent's file reference**
Jg-2451-PCT

**IMPORTANT NOTIFICATION**

**International application No.**
PCT/GB00/01354

**International filing date** (day/month/year)
10 April 2000 (10.04.00)

**1.** The following indications appeared on record concerning:

[X] the applicant [ ] the inventor [ ] the agent [ ] the common representative

Name and Address
TELEPATHIC INDUSTRIES LTD.
37 Station Road
London NW4 4PN
United Kingdom

State of Nationality: GB
State of Residence: GB
Telephone No.:
Facsimile No.:
Teleprinter No.:

**2.** The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[X] the person [X] the name [X] the address [ ] the nationality [ ] the residence

Name and Address
ENFORMATICA LIMITED
Unit B
Chelford Court
Robjohns Road
Chelmsford
Essex CM1 3AG
United Kingdom

State of Nationality: GB
State of Residence: GB
Telephone No.:
Facsimile No.:
Teleprinter No.:

**3.** Further observations, if necessary:

**4.** A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

**The International Bureau of WIPO**
**34, chemin des Colombettes**
**1211 Geneva 20, Switzerland**
Facsimile No.: (41-22) 740.14.35

Authorized officer
Idhir BRITEL
Telephone No.: (41-22) 338.83.38

14

PATENT COOPERATION TREATY

PCT



# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

## (PCT Article 36 and Rule 70)

| Applicant's or agent's file reference | FOR FURTHER ACTION | See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416) |
|---|---|---|
| Jg-2451-PCT | | |
| International application No. | International filing date *(day/month/year)* | Priority date *(day/month/year)* |
| PCT/GB00/01354 | 10/04/2000 | 26/04/1999 |
| International Patent Classification (IPC) or national classification and IPC<br>H04L9/32 | | |
| Applicant<br>TELEPATHIC INDUSTRIES LTD. et al. | | |

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

| Date of submission of the demand | Date of completion of this report |
|---|---|
| 09/11/2000 | 23.07.2001 |
| Name and mailing address of the international preliminary examining authority:<br>European Patent Office<br>D-80298 Munich<br>Tel. +49 89 2399 - 0 Tx: 523656 epmu d<br>Fax: +49 89 2399 - 4465 | Authorized officer<br>Apostolescu, R<br>Telephone No. +49 89 2399 7950 |

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB00/01354

## I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:
**Description, pages:**

| | | | | | |
|---|---|---|---|---|---|
| 1-11 | as originally filed | | | | |

**Claims, No.:**

| | | | | | |
|---|---|---|---|---|---|
| 1-9 | as received on | 08/05/2001 | with letter of | 08/05/2001 | |

**Drawings, sheets:**

| | | | | | |
|---|---|---|---|---|---|
| 1/1 | as originally filed | | | | |

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   - ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
   - ☐ the language of publication of the international application (under Rule 48.3(b)).
   - ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   - ☐ contained in the international application in written form.
   - ☐ filed together with the international application in computer readable form.
   - ☐ furnished subsequently to this Authority in written form.
   - ☐ furnished subsequently to this Authority in computer readable form.
   - ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   - ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   - ☐ the description, pages:
   - ☐ the claims, Nos.:

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

   *(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)*

6. Additional observations, if necessary:

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

| | | | |
|---|---|---|---|
| Novelty (N) | Yes: | Claims | 1-8 |
| | No: | Claims | |
| Inventive step (IS) | Yes: | Claims | 1-8 |
| | No: | Claims | 9 |
| Industrial applicability (IA) | Yes: | Claims | 1-9 |
| | No: | Claims | |

2. Citations and explanations
   **see separate sheet**

## VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:
**see separate sheet**

Re Item V

**Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

Reference is made to the following documents:

D1: US-A-5 499 294 (FRIEDMAN GARY L) 12 March 1996 (1996-03-12)
D2: US-A-5 801 856 (RABBANI MAJID ET AL) 1 September 1998 (1998-09-01)

**1. Independent claims 1 and 6.**

It is considered that claims 1 and 6 relate to new and inventive subject-matter (Articles 33 (2) and (3) PCT), since the prior art does not disclose or suggest the specifically claimed device for use in validating recorded digitized information according to claim 1 and does not disclose or suggest the specifically claimed process for use in validating recorded digitized information according to claim 6.

Document D1 discloses a digital camera equipped with a processor for authentication of images produced from an image file taken by the camera.
The camera processor has embedded therein a private key unique to it and the camera housing has a public key that is so uniquely related to the private key that digital data encrypted with the private key may be decrypted using the public key. The processor calculates a hash of the image file using a predetermined algorithm and encrypts the image hash with the private key to produce a digital signature. To further enhance the authenticatableness of the image, information is added in a border of the camera image frame, such as the public key which is a unique serial number identifying the camera, the date, time, latitude and longitude of the camera position. All of the added information that is recorded in the border of the image frame is hashed and encrypted together with the image to become part of the signature.
The invention described in document D2 is directed to a secure photographic system in which a security feature indicia instructs the photofinisher to apply a security feature, such as encryption for access control or a digital signature for authentication to the digital image.

Claim 1 of the present invention relates to a device for use in securing and preserving evidence from computers and listening devices. The device produce a data file for recording on recording media having a header and an enciphered message. The enciphered message is the recorded message enciphered with the date, time, serial number of the device and the geophysical location information indicative of the actual location of the device. The header contains the private key encrypted date, time, serial number and geophysical location information used in the cipher process.

Claim 6 of the present invention relates to the process for validating recorded digitized information. The process produces a data file of the recorded information enciphered with the date, time, serial number of the recording equipment and the geophysical location information. The process forms also a file header containing the private key encrypted date, time, serial number and geophysical location information used in the cipher process.

**2. Dependent claims 2 to 5, 7 and 8.**

Claims 2 to 5, 7 and 8 contain further details of the device of claim 1 and of the process of claim 6 respectively. As they are dependent on claims 1 and 6 respectively, they also satisfy the requirements for novelty and inventive step (Articles 33 (2) and (3) PCT).

**3. Independent claim 9.**

Document D1, which is considered to represent the most relevant state of the art, discloses a device for use in validating recorded digitised information (abstract), characterised in that the device generates an encrypted message arranged at the end of the recorded information (figure 3A and 3B), said encrypted message including the private key encrypted date, time and serial number and geophysical location of the device on which it was recorded (column 5 line 56 to 65, column 9 line 7 to 28, figure 4).

The subject-matter of claim 9 differs from this disclosure in that the encrypted message including the private key encrypted date, time, serial number and geophysical location of the unit on which is was recorded together with identification code of the recorded work, is sent over the short message system of a mobile telephone system to a third

party.

The problem to be solved by the present invention may therefore be regarded as how to communicate a secure validation of a recorded message to a third party.

The skilled person would regard it a normal design procedure to combine the features described in D1 with his general knowledge about communication networks and billing systems to overcome the problem posed.

Therefore the subject-matter of claim 9 does not involve an inventive step and does not satisfy the criterion set forth in Article 33(3) PCT.

Re Item VII

**Certain defects in the international application**

1. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1 and D2 is not mentioned in the description, nor are these documents identified therein.

2. Claim 9 contains the sign placed in parentheses "(SMS)". This sign is a definition of the respective feature, "short message system", and not a reference sign.
Only reference signs of the technical features are allowed to be placed in parentheses.

## CLAIMS

1. A device for use in validating recorded digitized information including voice, video, telemetry or computer generated information or the like, characterised in that the device includes a tamper-proof unit (TPB) accommodating means for identifying the date and time (RTC) and serial number of the device (SRN) in a cipher data register (CDR) and the private key (PCR) of a public key encryption pair allocated to the device, the device being arranged in operation to produce a data file for recording on standard recording media (RD) having a header (H-Data) and an enciphered message (DATA), the recorded message being enciphered by a cipher unit (CU) with the date, time and serial number held in the said cipher register (CDR) and the header (H-Data) contains the private key encrypted date, time and serial number used in the cipher process provided by an encryption unit (EU), and characterised in that the device includes a geophysical location defining unit (GU) for generating geophysical location information (C) indicative of the actual location of the device and said geophysical location information is used by the cipher unit (CU) to encipher the recorded message and is included by the encryption unit (EU) in the encrypted header (H-Data).

2. A device as claimed in claim 1 in which the geophysical location defining unit (GU) is a digital mobile telephone instrument of the type including a global positioning system.

3. A device as claimed in claim 2 in which the mobile telephone instrument (GU) includes a short message service system and every encrypted header (H-Data) is also sent to a trusted third party by way of the mobile telephone short message service.

4. A device as claimed in any preceding claim in which the encryption unit (EU) also creates a digital fingerprint for incorporation in the header (H-Data) comprising a unique value calculated from the message.

5. A device as claimed in any preceding claim in which an inbuilt location identifier (LI) is programmed with the actual geophysical location (PL) of the device and is arranged to inhibit the operation of the cipher unit (CU) and the encryption unit (EU) if the values of the actual geophysical location identifier (LI) and the geophysical location information (C) generated by the geophysical unit (GU) do not equate.

6. A process for use in validating recorded digitized voice, video, telemetry or digital computer generated information or the like, characterised in that the process produces a data file of the recorded information enciphered with the date, time and serial number of the recording equipment and forms a file header (H-Data) containing the private key encrypted date, time and serial number used in the enciphering process, and characterised in that the recorded information is also enciphered with geophysical location information which is also formed into the file header (H-Data).

7. A process as claimed in claim 6 in which the file header (H-Data) is sent to a trusted third party to validate enciphered recorded information and encrypted header.

8. A process as claimed in claim 6 or claim 7 in which the header also incorporates a digital fingerprint comprising a unique value calculated from the message.

9. A copyright management system for use with electronically distributed digital products such as music, video and multi-media works, characterised in that an electronic distribution system includes a set-top box which includes means for generating an encrypted message arranged at the end of a download by

the set top box to create an encrypted message including the private key encrypted date, time, serial number and geophysical location of the set top box together with identification code of the work downloaded for communication over the short message system (SMS) of a mobile telephone system to the electronic digital product distributor.

Replacement nce

PATENT COOPERATION TREATY

PCT

# INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

| Applicant's or agent's file reference | FOR FURTHER ACTION | see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below. |
|---|---|---|
| Jg-2451-PCT | | |
| International application No. | International filing date *(day/month/year)* | (Earliest) Priority Date *(day/month/year)* |
| PCT/GB 00/01354 | 10/04/2000 | 26/04/1999 |
| Applicant | | |
| TELEPATHIC INDUSTRIES LTD. | | |

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 1

   [X] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

# INTERNATIONAL SEARCH REPORT

International Application No
PC[redacted]B 00/01354

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

WPI Data, INSPEC, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 5 499 294 A (FRIEDMAN GARY L)<br>12 March 1996 (1996-03-12) | 1-3,7 |
| A | column 5, line 49 -column 6, line 19<br>column 7, line 6 - line 10<br>column 7, line 58 - line 65<br>column 9, line 8 - line 28 | 2,8 |
| | --- | |
| Y | US 5 801 856 A (RABBANI MAJID ET AL)<br>1 September 1998 (1998-09-01)<br>column 1, line 45 - line 63<br>column 2, line 11 - line 14<br>column 3, line 4 - line 12<br>column 3, line 24 - line 48<br>column 4, line 4 - line 10<br>column 4, line 20 - line 60 | 1-3,7 |
| | --- | |
| | -/-- | |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 11 August 2000 | 17 08 2000 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Holper, G |

2

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category ° | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | EP 0 715 241 A (MITSUBISHI CORP)<br>5 June 1996 (1996-06-05)<br>abstract<br>column 6, line 41 -column 7, line 3 | 11 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 00/01354

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 5499294 A | 12-03-1996 | NONE | |
| US 5801856 A | 01-09-1998 | NONE | |
| EP 0715241 A | 05-06-1996 | JP 8287014 A<br>US 5867579 A | 01-11-1996<br>02-02-1999 |

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/32

A1

(11) International Publication Number: WO 00/65771

(43) International Publication Date: 2 November 2000 (02.11.00)

(21) International Application Number: PCT/GB00/01354

(22) International Filing Date: 10 April 2000 (10.04.00)

(30) Priority Data:
9909590.3 26 April 1999 (26.04.99) GB

(71) Applicant *(for all designated States except US)*: TELEPATHIC INDUSTRIES LTD. [GB/GB]; 37 Station Road, London NW4 4PN (GB).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: KELMAN, Alistair, Bruce [GB/GB]; 37 Station Road, London NW4 4PN (GB).

(74) Agent: JONES, Graham, Henry; Graham Jones & Company, 77 Beaconsfield Road, Blackheath, London SE3 7LG (GB).

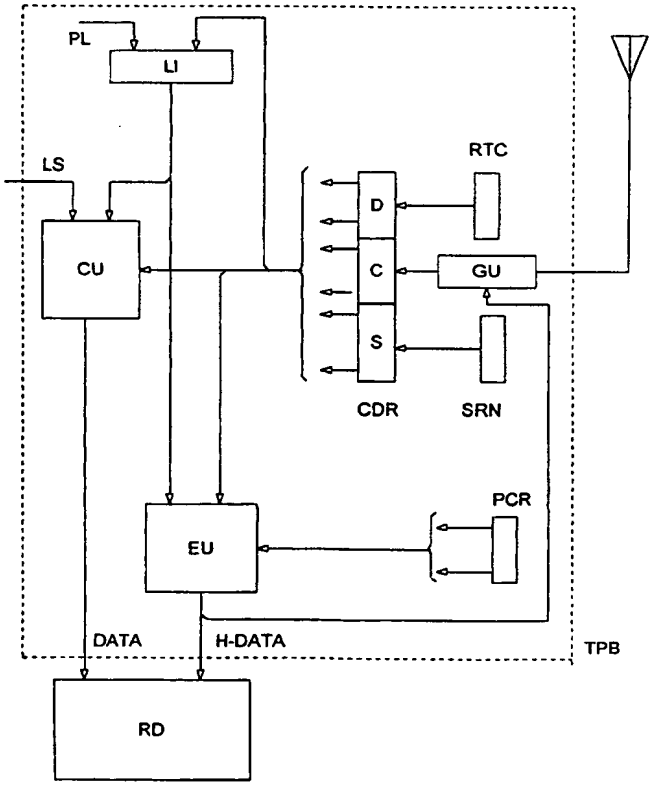
(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published**
*With international search report.*

(54) Title: MECHANISM FOR SECURING RELIABLE EVIDENCE FROM COMPUTERS AND LISTENING DEVICES

(57) Abstract

A device for use in securing and preserving evidence from computers and listening devices. The device includes a tamper proof unit accommodating date, time and device serial number identifying arrangements together with the private key of a Public Key encryption pair. The device being arranged in operation to produce a data file for recording on recording media having a header and an enciphered message. The enciphered message being the recorded message enciphered with the date, time and serial number of the device. The header containing the private key encrypted date, time and serial number used in the cipher process.



*FOR THE PURPOSES OF INFORMATION ONLY*

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **AL** | Albania | **ES** | Spain | **LS** | Lesotho | **SI** | Slovenia |
| **AM** | Armenia | **FI** | Finland | **LT** | Lithuania | **SK** | Slovakia |
| **AT** | Austria | **FR** | France | **LU** | Luxembourg | **SN** | Senegal |
| **AU** | Australia | **GA** | Gabon | **LV** | Latvia | **SZ** | Swaziland |
| **AZ** | Azerbaijan | **GB** | United Kingdom | **MC** | Monaco | **TD** | Chad |
| **BA** | Bosnia and Herzegovina | **GE** | Georgia | **MD** | Republic of Moldova | **TG** | Togo |
| **BB** | Barbados | **GH** | Ghana | **MG** | Madagascar | **TJ** | Tajikistan |
| **BE** | Belgium | **GN** | Guinea | **MK** | The former Yugoslav Republic of Macedonia | **TM** | Turkmenistan |
| **BF** | Burkina Faso | **GR** | Greece | | | **TR** | Turkey |
| **BG** | Bulgaria | **HU** | Hungary | **ML** | Mali | **TT** | Trinidad and Tobago |
| **BJ** | Benin | **IE** | Ireland | **MN** | Mongolia | **UA** | Ukraine |
| **BR** | Brazil | **IL** | Israel | **MR** | Mauritania | **UG** | Uganda |
| **BY** | Belarus | **IS** | Iceland | **MW** | Malawi | **US** | United States of America |
| **CA** | Canada | **IT** | Italy | **MX** | Mexico | **UZ** | Uzbekistan |
| **CF** | Central African Republic | **JP** | Japan | **NE** | Niger | **VN** | Viet Nam |
| **CG** | Congo | **KE** | Kenya | **NL** | Netherlands | **YU** | Yugoslavia |
| **CH** | Switzerland | **KG** | Kyrgyzstan | **NO** | Norway | **ZW** | Zimbabwe |
| **CI** | Côte d'Ivoire | **KP** | Democratic People's Republic of Korea | **NZ** | New Zealand | | |
| **CM** | Cameroon | | | **PL** | Poland | | |
| **CN** | China | **KR** | Republic of Korea | **PT** | Portugal | | |
| **CU** | Cuba | **KZ** | Kazakstan | **RO** | Romania | | |
| **CZ** | Czech Republic | **LC** | Saint Lucia | **RU** | Russian Federation | | |
| **DE** | Germany | **LI** | Liechtenstein | **SD** | Sudan | | |
| **DK** | Denmark | **LK** | Sri Lanka | **SE** | Sweden | | |
| **EE** | Estonia | **LR** | Liberia | **SG** | Singapore | | |

Title:

Mechanism for securing reliable evidence from computers and listening devices

Technical Field

This invention relates to methods and apparatus for securing and preserving evidence from computers and listening devices in a form which eliminates or reduces the need for corroborative or supporting evidence regarding the circumstances of the making of the recording.

Background

Throughout the history of computing it has been known that evidence from computers has been modifiable in most cases without trace. Modification and fabrication of computer evidence has led to serious problems in the investigation and prosecution of computer crimes, in the management of computer security, in the keeping of business records in accordance with the security provisions of the Companies Acts and in the cost of litigation where evidence has been derived from computers.

In criminal investigations the reliability of evidence from computers has had to be secured by complex administrative procedures ("bagging and tagging") when freezing computer evidence at the scene of an alleged crime together with the use of image copying equipment to take bit image copies of suspected computer systems. Police officers and computer staff have had to give detailed evidence regarding how they secured computer systems and preserved the computer evidence. In managing computer security there have been cases where it has been difficult or impossible to show precisely what data or programs were on particular computer systems at particular times. In the keeping of business records there have concerns about the conversion of paper records into document image copies and their subsequent reliability as contemporaneous evidence. One security concern has been the fact that a document image copy can be used to create modified versions of itself which cannot be

shown to be forgeries without a very expensive forensic examination being undertaken - and sometimes with it being impossible to prove that the document image is an unmodified original. Consequently expensive administrative controls regarding the storage of document image copies are necessary to maintain adequate security.

Additionally police and security services have made greater use of listening devices under warrant for the monitoring of suspected criminals. Currently under UK legislation the evidence from such listening devices can only be used for intelligence gathering purposes and cannot be tendered in evidence in civil or criminal trials. This situation is presently under review and it is anticipated that UK law will be changed to allow for evidence from listening devices under warrant to be admissible in civil and criminal trials in certain circumstances. Concern has been expressed regarding the need for security services personnel to testify regarding the planting of listening devices and their compliance with administrative procedures to secure the reliability of evidence from listening devices.

Object of the Invention

It is an object of the invention to provide a computer peripheral, termed the "DataFreeze", which will automatically secure evidence in a form which will be accepted as being electronically "bagged and tagged" - that is to say the evidence will be encapsulated in a form which establishes precisely when it was obtained and where it was obtained.

According to the invention there is provided a device for use in validating recorded digitised voice, video, telemetry or computer generated information or the like, characterised in that the device includes a tamper-proof unit accommodating means for identifying the date, time and serial number of the device and the private key of a Public key encryption pair allocated to the device, the device being arranged in operation to produce a data file for recording on recording media having a header and an enciphered message, the recorded message being enciphered with the date, time and

serial number of the device and the header containing the private key encrypted date, time and serial number used in the cipher process.

According to the invention there is provided a process for use in validating recorded digitised voice, video, telemetry or digital computer generated information or the like, in which the process produces a data file of the recorded information enciphered with the date, time and serial number of the recording equipment and forms a file header containing the private key encrypted date, time and serial number used in the enciphering process.

According to a feature of the invention the cipher process and encrypted header also include geophysical location information indicative of the actual location of the device making the validated recording.

The device according to the invention may be a micro-processor controlled arrangement and the process of the invention may be performed by a computer program.

The equipment of the invention performs these operations in real-time without adding any significant delay to the recording of the data, without the need for a powerful encryption microprocessor and without the need for skilled personnel. Once the recording has been secured and encapsulated by the DataFreeze hardware the resulting disk, tape, electronic recording, magnetic recording or optical recording is re-playable on any conventional replay device for the replay of that type of media running special DataFreeze deciphering software. Consequently, in one possible implementation, a prosecuting authority could supply to an accused's lawyers with a CDROM produced by the arresting officers on a DataFreeze peripheral which was readable by the accused's lawyers on their conventional windows personal computer with the DataFreeze decryption/deciphering software running. No additional hardware would be required by the defence lawyers. The date, time, geophysical or CURSOR location and serial number of the DataFreeze peripheral used to make the recording would

however always be available to the defence in confirmation of when, where and on what equipment the data had been frozen by the police or security forces.

Outside of the police and security services a DataFreeze peripheral could be used as an archival storage device in banking and financial services or as a tachograph or other work monitoring device in medical and in health and safety applications.

Description of one embodiment of the invention

One embodiment of the invention will be described with reference to the accompanying drawing.

The manufacturer, DataFreeze, generates a Public Key encryption pair for each unit to be manufactured - the public key being published as an X500 Digital Certificate and the private key being kept secret. Each private key is built into a private key register PCR on a custom chip in a tamper-proof module TPB. Inside a DataFreeze peripheral is the custom chip in a tamper-proof module TPB which is connected to a standard recording device RD (e.g. A CDROM writer or a floppy disk drive). The custom chip embodies a micro-processor and contains a geophysical positioning system GU (in one implementation of the invention a CURSOR mobile telephone positioning system), a real-time clock RTC and a unique serial number SRN. The output from these three devices, in one possible implementation, is converted into a 512 bit number with the left portion containing the data and time D, the middle containing the positioning system's location (the CURSOR location) C and the right portion containing the Serial Number S in a cipher data register CDR.

Within the custom chip the 512 bit number in the cipher data register CDR is encrypted using the private key from the private key register PCR of the particular unit in the encryption unit EU. The resulting encrypted stream is called "H-Data". Because the volume of data (512 bits) being encrypted by the private key is very small, the vulnerability of the data to cryptoanalysis to discover the private key is very low.

To start a recording session the DataFreeze unit receives data from an external source LS (line under Surveillance) (e.g. a computer or a listening device). The DataFreeze unit notes the "H-Data" and writes this to the recording media RD as a header to the recording, padding any spare space in the header with zeros.

The DataFreeze unit now takes the first block of data received from the external source stored in the cipher unit CU. It performs three simple Caesar cipher operations on the block of data e.g. Multiplying the block of data by the new date and time and adding the cursor location and the square of the serial number.

i.e. DataFreeze block =([Data]*D1) + C+(S*S)

For the next block of data it performs a different calculation e.g. Multiplying the block of data by the CURSOR location, adding the square of the new date and time (which will have increased a defined amount during the writing of the first block) and adding the serial number.

i.e. DataFreeze block =([Data]*C) + (D2*D2)+S

For the next block of data it performs a different calculation e.g. Multiplying the block of data by the square of the serial number, adding the square of the CURSOR location and adding the new date and time (which will have increased a defined amount during the writing of the second block).

i.e. DataFreeze block =([Data]*S*S) + D3+C

For the fourth block of data the DataFreeze peripheral would revert to enciphering using the algorithm used for the first block of data.

i.e. DataFreeze block =([Data]*D4) + C+S

Further variations on this manipulation are possible. However particular care must be taken in selection of the manipulations to avoid floating point operations which are

likely to introduce floating point precision errors in the calculation when this is performed on conventional microprocessors.

The objective of the DataFreeze enciphering is not to make the data cryptographically secure i.e. secret. Rather it is to freeze the data as recorded with the date and time when it was recorded, the location where it was recorded and the unit on which it was recorded. For proof of no tampering it has to do this in real-time. The simple manipulations of data are performed in a few cycles of the microprocessor running on the DataFreeze peripheral and cause no material delay in the writing of the data.

To replay a DataFreeze recording on a standard replay device the computer controlling the device would run the DataFreeze decryption/deciphering software. This would read the "H-data" from the header and decrypt it using the DataFreeze public key, which would be published as an X500 digital certificate. Once the header had been decrypted the left, middle and right portions of the header would be stored in buffers and used as the seed data for a computer program to step through the obverse of the enciphering process. Thus in the suggested implementation - the first block of DataFreeze data would have the CURSOR location subtracted and the square of the serial number subtracted with the result being divided by the date and time.

i.e. Data - ([DataFreeze Data] - C -(S*S))/D1

The second block of DataFreeze data would have the square of the new date and time (which will have increased a defined amount during the writing of the first block) subtracted, the serial number subtracted and the result divided by the CURSOR location.

i.e. Data = ([DataFreeze Data] - D2 -S)/C

The third block of data would have the square of the CURSOR location subtracted, the new date and time (which will have increased a defined amount during the writing

of the second block) subtracted and the result divided by the square of the serial number.

i.e. Data = ([DataFreeze Data] - (C*C) -D3)/(S*S)

Such simple mathematical processes would not lead to any material overhead in the outputting of the data. It would also be possible to 'fast forward' and 'reverse' along a DataFreeze recording by noting the block number from the header and cycling through to the predicted algorithm, date and time, CURSOR location and serial number.

With sufficient computing power and time it would always be possible to decipher a DataFreeze recording which had lost its header by trying various combinations of date, location and serial number against the fragment of the recording. However because the H-Data is digitally signed using the private key of the DataFreeze X500 digital certificate of the particular unit and the private key is located within a tamper proof module within the CURSOR unit along with the real time clock it would not be possible to create a fabricated DataFreeze recording which predated the original since this would require the forgery of the cryptographically secure H-data in the header.

A more sophisticated version of the invention could include a "digital fingerprint" in the header along with the H-Data. This would be produced by simultaneously passing a duplicate of the entire data session through a one-way algorithm while it was being written to disk to produce a unique value known as a message digest which would, in effect, be a "digital fingerprint" of the session. This message digest could then be encrypted by the DataFreeze unit's private key and written to the header field H-data of the recording. When decrypted in software by using the DataFreeze unit's X500 public key this message digest could be used to confirm the integrity and coherence of the recording of the data session.

A further version of the invention could contain a dummy or non-functional CURSOR unit located in the tamper-proof module. This would not determine the location of the

unit but would simply give out a default location for inclusion in the H-Data. The DataFreeze unit would thus only stamp the data with the time and specific unit and the default location. Such a unit would have two main uses: Use in situations where it was not possible to get a location signal and use in situations where the cost of the DataFreeze unit needed to be low and the location information was not considered to be important.

In yet a further version of the invention the geophysical information may be used to control the use of the recording equipment by having an inbuilt location identifier LI which is programmable (i.e. lead PL is set with the geophysical location of the device) and is used to prevent use of the recording equipment if it is located outside the geophysical area indicated by the inbuilt location identifier LI by inhibiting the cipher unit CU and encryption unit EU if the values of PL and C do not equate. Typically the geophysical positioning unit may be the Global positioning system used in mobile telephones by including a complete mobile telephone instrument in the Position Unit GU.

Preferably the standard recording medium is of the "Write once read many times" type where it is impossible to purge a record once it has been written. However, the invention may be used with erasable media.

To overcome the security vulnerability of erasable media it is necessary to have a mechanism that detects deletions from the stored information. To ensure that such a deletion is detectable it is possible to arrange that the encrypted header H-data produced by the encryption unit EU of every document stored using DataFreeze is sent using the mobile cellphone incorporated into the position unit GU supplying the location information using a Short Message Service SMS message. This would provide an audit trail logged by a Trusted Third Party which could be compared with the electronic copy. If a document were purged on the erasable media its omission

would be obvious since the two sets of records, the SMS logs and the encrypted headers on the local copy would not be identical.

The invention has application beyond that involving criminal investigation. For example in the publishing industry copyright rights are traditionally allocated by physical territories. Thus a copyright owner can license one publisher to publish his work in a specific territory (e.g. USA) and another publisher to publish his work in a different territory (e.g. Europe) each paying different royalties. The ability to segregate territories is important for copyright owners to maximise their income through taking account of the relative wealth of particular territories. Thus the author of a book on soil science might reasonably wish to sell his book at $15 a copy to people living in a wealthy country (E.g. USA) and at $0.50 per copy to people living in a poor country (e.g. Cambodia) and make the material available free to a charitable foundation. An enhancement of the DataFreeze technology makes such a segregation possible.

In this implementation the DataFreeze unit according to the invention becomes part of a media recording device (e.g. a set top box supplied by a media company). Under this amended system the SMS message transmitted would consist of five parts: the normal encrypted DataFreeze header (with check sum to prove that the recording was complete); the ISBN (or equivalent) of the downloaded work (thereby identifying the work), the Location Information, the serial number of the set-top box and the date & time of download. These five parts would be encrypted using the public key of the set-top box maker.

By way of example instead of using a book we will consider the downloading of a pay-per-view music video. The consumer wishing to download the pay-per-view music video would instruct his unit to download it. At the end of the download the set-top box would send the encrypted SMS message to the media company. This message would be stored and from time to time (e.g. daily, weekly or monthly) the batches of

SMS messages would be decrypted using the private key of the media company thereby generating the DataFreeze header (proving that the material was successfully downloaded), the ISDN number (identifying the work downloaded), the Location Information (therefore establishing the territory in which the work was downloaded and consequently the amount of royalties due as well as the duty and consumption taxation due on the transaction), the serial number of the set-box (thereby establishing who to send the bill to) and the data and time of download (thereby establishing the period for billing purposes and also essential as billing information when the price due for the download varies over time).

Based upon the SMS data received the consumer would be sent (or directly debited) with his bill for the materials downloaded by his set-box and the media company would be able to account to the copyright owner and the national government for royalties, duty and taxes due for downloading in the territory where the set-top box was located. So if the set top box was registered to a charity in a specific location it would be possible for the bills to be waived.

One very specific advantage of this kind of system is that it contains within it protection against piracy. Any person using a DataFreeze set-top box for downloading would be identifying their physical location, necessary for the proper accounting of royalty payments, duty and taxes. If a set-top box was stolen the consumer would report the loss to the media company. Any download which occurred thereafter would give the new location of the stolen box, thereby assisting in the arrest and prosecution of the thief. Because the SMS message is encrypted using the private key of the media company, so long as this private key remains secure, there is no means by which the location information, the ISBN and the serial number of the unit could be falsified. However like all digital signature systems the security of the rights management system depends upon the private key being kept secret - consequently the company which generates and supplies the media company with its private and public key pair must be as trustworthy as a bank note supplier to governments.

One further variant on all forms of the DataFreeze unit according to the invention could have a biometric sensor attached to the unit. In this enhancement when a recording were to be made the biometric sensor would check the relevant biometric of the user (e.g. the fingerprint). If it found this to be valid it would then encrypt the DataFreeze header data with the private key associated with the user. This re-encrypted DataFreeze header would be written to the unit and, in an enhanced version, sent by SMS to the external store for audit purposes.

In this variant the decryption process has one further stage. Before commencing to decrypt the DataFreeze header encrypted in the way set out the original patent application the DataFreeze software would have to obtain the public key associated with the user. Using this public key it would decrypt the message to reveal the original encrypted DataFreeze header. Using the public key of the recording device the unit would then decrypt the DataFreeze header itself revealing the date, location, serial number (and checksum).

Both the user's public keys and the recording devices public keys could be obtained from a web site. In this implementation a further header could preceded the DataFreeze header on the recording giving the URLs of the public key of the user and the public key of the recording device. In regular use this information could be downloaded and cached so that no material delay would occur when reading records produced by people or devices in frequent correspondence with each other.

All of the enhancements and variations identified above can be implemented by a suitably programmed micro-processor.

CLAIMS

1. A device for use in validating recorded digitised information including voice, video, telemetry or computer generated information or the like, characterised in that the device includes a tamper-proof unit (TPB) accommodating means for identifying the date and time (RTC) and serial number of the device (SRN) in a cipher data register (CDR) and the private key (PCR) of a public key encryption pair allocated to the device, the device being arranged in operation to produce a data file for recording on standard recording media (RD) having a header (H-Data) and an enciphered message (DATA), the recorded message being enciphered by a cipher unit (CU) with the date, time and serial number held in the said cipher data register (CDR) and the header (H-Data) contains the private key encrypted date, time and serial number used in the cipher process provided by encryption unit (EU).

2. A device as claimed in claim 1 in which a geophysical location defining unit (GU) is included generating geophysical location information (C) indicative of the actual location of the device and said geophysical location information is used by the cipher unit (CU) to encipher the recorded message and is included by the encryption unit (EU) in the encrypted header (H-Data).

3. A device as claimed in claim 2 in which the geophysical location defining unit (GU) is a digital mobile telephone instrument of the type including a global positioning system.

4. A device as claimed in claim 3 in which the mobile telephone instrument (GU) includes a short message service system and every encrypted header (H-Data) is also sent to a trusted third party by way of the mobile telephone short message service.

5. A device as claimed in any preceding claim in which the encryption unit (EU) also creates a digital fingerprint for incorporation in the header (H-Data) comprising a unique value calculated from the message.

6. A device as claimed in claim 2, 3, 4 or 5 in which an inbuilt location identifier (LI) is programmed with the actual geophysical location (PL) of the device and is arranged to inhibit the operation of the cipher unit (CU) and the encryption unit (EU) if the values of the actual geophysical location identifier (LI) and the geophysical location information (C) generated by the geophysical unit (GU) do not equate.

7. A process for use in validating recorded digitised voice, video, telemetry or digital computer generated information or the like, in which the process produces a data file of the recorded information enciphered with the date, time and serial number of the recording equipment and forms a file header containing the private key encrypted date, time and serial number used in the enciphering process.

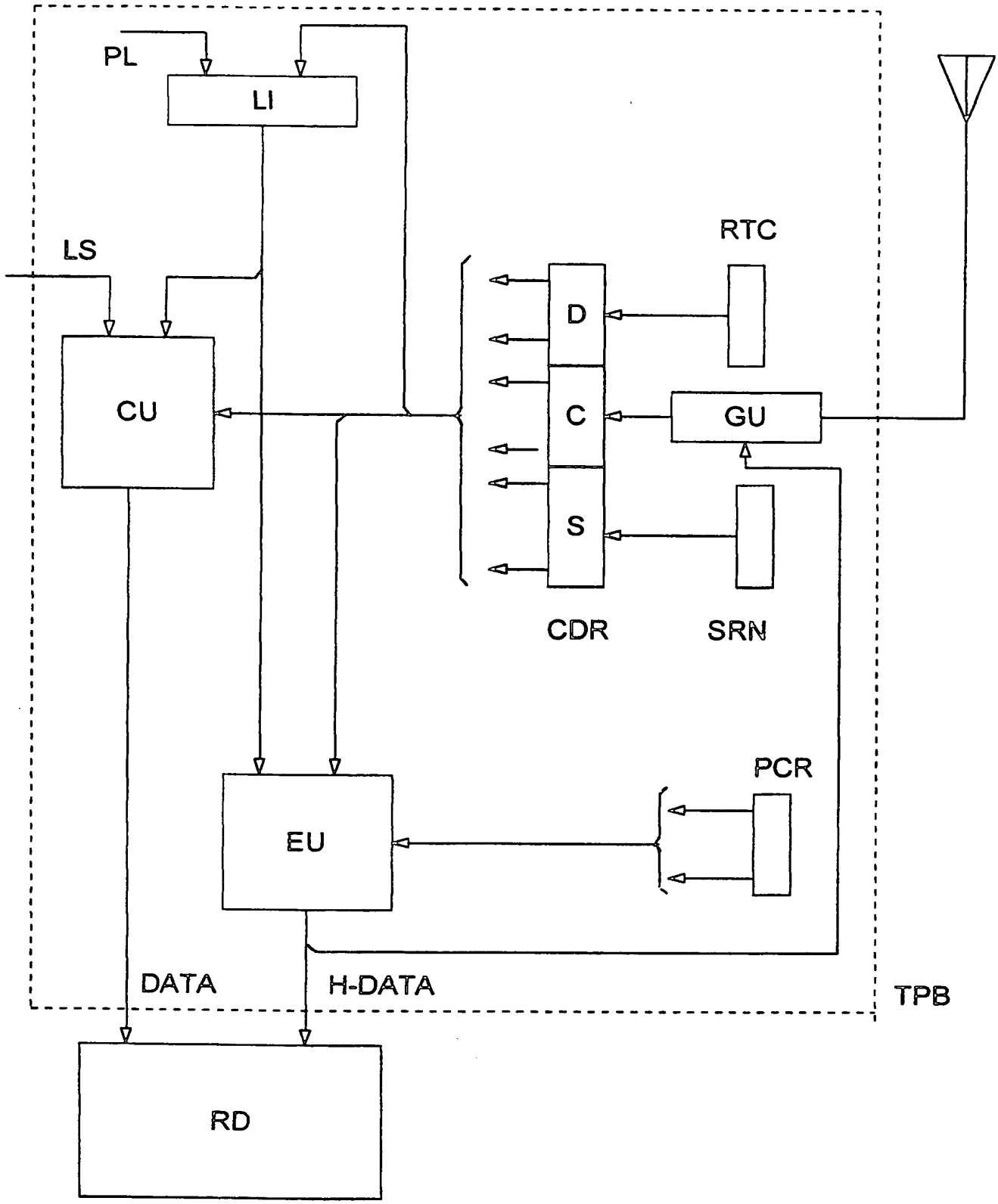
8. A process as claimed in claim 7 in which the recorded information is also enciphered with geophysical location information which is also formed into the file header.

9. A process as claimed in claim 7 in which the file header is sent to a trusted third party to validate enciphered recorded information and encrypted header.

10. A process as claimed in claims 7 to 9 in which the header also incorporates a digital fingerprint comprising a unique value calculated from the message.

11. A copyright management system for use with electronically distributed digital products such as music, video and multi-media works in which electronic distribution system includes a set-top box which includes means for generating an encrypted message arranged at the end of a download by the set top box to

create an encrypted message including the private key encrypted date, time, serial number and geophysical location of the set top box together with identification code of the work downloaded for communication over the short message system of a mobile telephone system to the electronic digital product distributor.


PL
LI
LS
CU
RTC
D
C
S
GU
CDR
SRN
EU
PCR
DATA
H-DATA
TPB
RD